CLAIMS

1. A method for rights management of digital content and secure delivery of digital content documents from a publisher site to an unsecure site, the method comprising:
   (a) encrypting each digital content document at the publisher site with a key to generate encrypted document content;
   (b) computing for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document;
   (c) creating a list of document identifier and decryption key pairs;
   (d) assembling the encrypted document content for each content document and the list into a distribution archive;
   (e) encrypting the distribution archive with a scheduled key;
   (f) installing a content server at the unsecure site; and
   (g) sending the distribution archive from the publisher site to the content server.

2. The method of claim 1 wherein step (a) comprises compressing each document before encrypting the document.

3. The method of claim 1 wherein step (b) comprises computing a document identifier from the encrypted document content and a text string at the publisher site.

4. The method of claim 1 further comprising:
   (h) at the unsecure site, decrypting the distribution archive with the scheduled key, extracting the encrypted document content and storing the encrypted document content in a storage located at the unsecure site.

5. The method of claim 4 wherein a user at the unsecure location accesses the content server from a browser and wherein the method further comprises:

(i) downloading a secure viewer program into the browser;

(j) using the viewer program to request a document from the content server;

(k) downloading an encrypted version of the requested document from the content server to the viewer; and

(l) using the viewer to calculate a document identifier from the encrypted version of the requested document and to send the document identifier to the content server.

6. The method of claim 5 further comprising:

(m) using the document identifier in the content server to retrieve a decryption key from the list and downloading the decryption key to the viewer program; and

(n) using the downloaded key in the viewer program to decrypt the encrypted version of the document and present the document to the user.

7. The method of claim 1 further comprising:

(h) monitoring content access at the unsecure site; and

(i) creating a log file at the unsecure site from the monitored activities.

8. The method of claim 7 further comprising:

(j) sending the log file to the publisher site in return for a distribution archive containing new content.

9. The method of claim 8 further comprising:

(k) extracting the contents of the log file at the publisher site;

(l) formatting the extracted contents and providing a report from the formatted contents to a reporting client.

10. The method of claim 7 wherein step (h) comprises monitoring user activities including login to the system, registration, creation of a user profile and the reading and printing of selected content documents.

11. Apparatus for rights management of digital content and secure delivery of digital content documents from a publisher site to an unsecure site, the apparatus comprising:

means for encrypting each digital content document at the publisher site with a key to generate encrypted document content;

an OID calculator that computes for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document;

means for creating a list of document identifier and decryption key pairs;

means for assembling the encrypted document content for each content document and the list into a distribution archive;

an encryptor that encrypts the distribution archive with a scheduled key;

means for installing a content server at the unsecure site; and

means for sending the distribution archive from the publisher site to the content server.

12. The apparatus of claim 11 wherein the means for encrypting each digital content document comprises a compressor that compresses each document and an encryption engine that encrypts the compressed document.

13. The apparatus of claim 11 wherein the OID calculator comprises means for computing a document identifier from the encrypted document content and a text string at the publisher site.

14. The apparatus of claim 11 further comprising a decryption engine located at the unsecure site that decrypts the distribution archive with the scheduled key, a file decompressor that extracts the encrypted document content and stores the encrypted document content in a storage located at the unsecure site.

15. The apparatus of claim 14 wherein a user at the unsecure location accesses the content server from a browser and wherein the apparatus further comprises means for downloading a secure viewer program into the browser, means for using the viewer program to request a document from the content server; means for downloading an encrypted version of the requested document from the content server to the viewer; an OID calculator in the viewer that calculates a document identifier from the encrypted version of the requested document and means for sending the document identifier to the content server.

16. The apparatus of claim 15 further comprising means for using the document identifier in the content server to retrieve a decryption key from the list, means for downloading the decryption key to the viewer program and means for using the downloaded key in the viewer program to decrypt the encrypted version of the document and present the document to the user.

17. The apparatus of claim 11 further comprising a log server that monitors content access at the unsecure site and means for creating a log file at the unsecure site from the monitored activities.

18. The apparatus of claim 17 further comprising means for sending the log file to the publisher site in return for a distribution archive containing new content.

19. The apparatus of claim 18 further comprising a reporting server that extracts the contents of the log file at the publisher site, formats the extracted contents and provides a report from the formatted contents to a reporting client.

20. The apparatus of claim 17 wherein the log server comprises means for monitoring user activities including login to the system, registration, creation of a user profile and the reading and printing of selected content documents.

21. A computer program product for rights management of digital content and secure delivery of digital content documents from a publisher site to an unsecure site, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code for encrypting each digital content document at the publisher site with a key to generate encrypted document content;

program code for computing for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document;

program code for creating a list of document identifier and decryption key pairs;

program code for assembling the encrypted document content for each content document and the list into a distribution archive;

program code for encrypting the distribution archive with a scheduled key;

program code for installing a content server at the unsecure site; and

program code for sending the distribution archive from the publisher site to the content server.

22. The computer program product of claim 21 wherein the program code for encrypting each digital content document at the publisher site comprises program code for compressing each document before encrypting the document.

23. The computer program product of claim 21 wherein the program code for computing a document identifier comprises program code for computing a

document identifier from the encrypted document content and a text string at the publisher site.

24. The computer program product of claim 21 further comprising program code at the unsecure site, for decrypting the distribution archive with the scheduled key, extracting the encrypted document content and storing the encrypted document content in a storage located at the unsecure site.

25. The computer program product of claim 24 wherein a user at the unsecure location accesses the content server from a browser and wherein the computer program product further comprises:

program code for downloading a secure viewer program into the browser;

program code in the viewer program for requesting a document from the content server;

program code for downloading an encrypted version of the requested document from the content server to the viewer; and

program code in the viewer for calculating a document identifier from the encrypted version of the requested document and for sending the document identifier to the content server.

26. The computer program product of claim 25 further comprising:

program code for using the document identifier in the content server to retrieve a decryption key from the list and downloading the decryption key to the viewer program; and

program code for using the downloaded key in the viewer program to decrypt the encrypted version of the document and present the document to the user.

27. The computer program product of claim 21 further comprising:

program code for monitoring content access at the unsecure site; and

program code for creating a log file at the unsecure site from the monitored activities.

28. The computer program product of claim 27 further comprising:

program code for sending the log file to the publisher site in return for a distribution archive containing new content.

29. The computer program product of claim 28 further comprising:

program code for extracting the contents of the log file at the publisher site;

program code for formatting the extracted contents and providing a report from the formatted contents to a reporting client.

30. The computer program product of claim 27 wherein the program code for monitoring content access comprises program code for monitoring user activities including login to the system, registration, creation of a user profile and the reading and printing of selected content documents.